

EQUATIONS FOR SUPERELLIPTIC CURVES OVER THEIR MINIMAL FIELD OF DEFINITION

LUBJANA BESHAI

*Department of Mathematics and Statistics
Oakland University
Rochester, MI, 48386.
Email: beshaj@oakland.edu*

FRED THOMPSON

*Department of Mathematics and Statistics
Oakland University
Rochester, MI, 48386.
Email: fjthomps@oakland.edu*

ABSTRACT. Let \mathcal{X}_g be a genus $g \geq 2$ superelliptic curve, F its field of moduli, and K the minimal field of definition. In this short note we construct an equation of the curve \mathcal{X}_g over its minimal field of definition K when \mathcal{X}_g has extra automorphisms. We make use of the dihedral invariants of superelliptic curves as defined by Shaska in [6] and results on the automorphism groups of superelliptic curves as in [10].

1. INTRODUCTION

Given an algebraic curve \mathcal{X} of genus $g \geq 2$, it is an open problem to determine an equation for \mathcal{X} over its minimal field of definition K . It is well known that the minimal field of definition is an algebraic extension of the field of moduli F . While for small genus it is known how to construct such equations, in general this is still an open problem. The overall strategy is to describe the point in the moduli space \mathcal{M}_g corresponding to the given curve. This determines the field of moduli F and the minimal field of definition K is a finite extension of the field of moduli. However, describing the moduli point explicitly can be done only for superelliptic curves of small genus; see [1–3].

Superelliptic curves are curves with affine equation $y^n = f(x)$. Such curves have at least an automorphism of order n . The quotient by the automorphism group of such curves is a genus 0 curve, hence a conic. This conic always has a rational point over a quadratic extension of the field of moduli. Hence, for superelliptic curves

2000 *Mathematics Subject Classification.* 11G30 and 11G50 and 14G40.

Key words and phrases. superelliptic curves and field of moduli and minimal field of definition and Shaska invariants.

$[K : F] \leq 2$. If the automorphism group of \mathcal{X} is isomorphic to the cyclic group of order n then an idea of Clebsch can be extended to determine if the field of moduli is a field of definition. Moreover an equation can be determined over the minimal field of definition. This is intended in [5].

When the superelliptic curves have extra automorphisms, i.e. the automorphism group has size $> n$ then the algorithm suggested above does not work. The isomorphism classes of such curves are determined by dihedral invariants (or Shaska invariants) as in [4, 8, 9].

In this short note we give an equation of superelliptic curves of genus $g \geq 2$ with extra automorphisms over the minimal field of definition K and determine the algebraic conditions in terms of such invariants of curves when the field of moduli is a field of definition.

Our main result is the following. Let \mathcal{X} be a genus $g \geq 2$ superelliptic curve, defined over \mathbb{C} , with an extra automorphism, $\mathfrak{s}_1, \dots, \mathfrak{s}_g$ its dihedral invariants, F the field of moduli, and K its minimal field of definition. Then,

- i) The minimal field of definition K is $K = F(\sqrt{\Delta_s})$
- ii) The equation of \mathcal{X} over K is

$$y^n = A x^{\delta(s+1)} + A x^{\delta s} + \sum_{i=1}^{s-1} 2^{s-i} \mathfrak{s}_1 \cdot \frac{\mathfrak{s}_s^i \mathfrak{s}_i - A \mathfrak{s}_{s+1-i}}{2^s \mathfrak{s}_1^2 - \mathfrak{s}_s^{s+1}} \cdot x^{\delta \cdot i} + 1$$

where

$$2^{s+1} A^2 - 2^{s+1} \mathfrak{s}_1 A + \mathfrak{s}_s^{s+1} = 0.$$

and Δ_s is the discriminant of the above quadratic,

$$\Delta_s = 2^{s+1} (2^{s+1} \mathfrak{s}_1^2 - 4 \mathfrak{s}_s^{s+1}).$$

Hence, this provides an Weierstrass equation of the curve over $k(\sqrt{\Delta_s})$.

An immediate consequence of the above result is that the field of moduli is a field of definition when the above quadratic has rational solutions. This happens if and only if Δ_s is a complete square.

It was noted in [9] that when Δ_s the automorphism group of the curve is larger and can be explicitly determined. The case when the genus g is odd differs from the case when it is even. As a corollary we get that if $\Delta_s = 0$ then the field of moduli is a field of definition as noted in [9] for hyperelliptic curves.

The results of this paper determine when the field of moduli is a field of definition and give an equation of the curve over the minimal field of definition for almost all superelliptic curves with extra automorphism. The next natural thing to study is the case of the generic superelliptic curve, that is the curves with equation $y^n = f(x)$ and automorphism group of order $n > 2$. Such algorithm is given in [7] for genus $g = 2$ and it is intended in [5] for all superelliptic curves.

2. PRELIMINARIES

Let \mathcal{X}_g be a genus $g \geq 2$ curve with full automorphism group $G = \text{Aut}(\mathcal{X}_g)$. The curve \mathcal{X}_g is called a **superelliptic curve** if there exists an element $\tau \in G$ which is central in G and $g(\mathcal{X}_g / \langle \tau \rangle) = 0$. Denote by H the cyclic group generated by τ , $H = \langle \tau \rangle$. Thus, $\bar{G} = G/H$ is called the reduced automorphism group of \mathcal{X}_g with respect to H .

Superelliptic curves are curves with affine equation $y^n = f(x)$. Denote with $K = k(x, y)$ the function field of \mathcal{X}_g and by $k(x)$ the genus zero subfield of K fixed by H . Then, $[K : k(x)] = n$, where $n = |H|$. The group \overline{G} is a subgroup of the group of automorphisms of a genus zero curve. Therefore, $\overline{G} < PGL_2(k)$ and \overline{G} is finite. Then, \overline{G} is isomorphic to one of the following groups C_m, D_m, A_4, S_4, A_5 . Since G is a degree n extension of \overline{G} and we know the possible groups that occur as \overline{G} , it is possible to determine G and the equation of K , see [10].

The group G acts on $k(x)$ via the natural way. The fixed field of this action is a genus 0 field, say $k(z)$. Thus, z is a degree $|G|$ rational function in x , say $z = \phi(x)$.

Given a superelliptic curve \mathcal{X}_g with equation $y^n = f(x)$ such that $\Delta(f, x) \neq 0$, the genus of the curve can be calculated using the following formula

$$g = 1 + \frac{1}{2} (nd - n - d - \gcd(d, n)).$$

where $\deg f = d > n$. If d and n are relatively prime then $g = \frac{(n-1)(d-1)}{2}$, see [11] for proof.

Much interesting to us are superelliptic curves with extra automorphism. Let \mathcal{X}_g be a superelliptic curve that has an extra automorphism $\sigma \in G$ such that its projection $\overline{\sigma} \in \overline{G}$ has order $\delta \geq 2$. Then the equation of the superelliptic curve is given as $y^n = g(x^\delta)$ or $y^n = xg(x^\delta)$, for some $g \in k[x]$, see [4] for proof. In other words \mathcal{X}_g has equation

$$y^n = g(x^\delta) := x^{s\delta} + a_{s-1}x^{(s-1)\delta} + \cdots + a_1x^\delta + 1,$$

or

$$y^n = xg(x^\delta) := x^{(s+1)\delta} + a_sx^{s\delta} + \cdots + a_1x^\delta + x.$$

For both cases the dihedral invariants of such curves or *Shaska-invariants* denoted by \mathfrak{s} -invariants are defined in [6, 8, 9]. They were discovered by Shaska in his thesis for curves of genus 2 with extra automorphisms and later generalized to all hyperelliptic curves in [9] for all hyperelliptic curves with extra automorphisms. Such invariants are used by many authors in computational aspects of hyperelliptic and superelliptic curves such as Duursma, Ritzenthaler, Lauter, Lercier, et al. We define them for our purposes in the next section.

3. EQUATION OF SUPERELLIPTIC CURVES AND DIHEDRAL INVARIANTS

Let \mathcal{X}_g be a superelliptic curve defined over a field k , $\text{char } k = 0$ such that \mathcal{X}_g has an extra involution and its Weierstrass equation is given by

$$(1) \quad y^n = x^{\delta(s+1)} + a_sx^{s\delta} + a_{s-1}x^{\delta(s-1)} + \cdots + a_2x^{\delta \cdot 2} + a_1x^\delta + 1$$

Our main goal is to find an equation of this curve defined over its minimal field of definition. The corresponding moduli point of such curves is determined by the dihedral invariants $\mathfrak{s}_1, \dots, \mathfrak{s}_s$ and the field of moduli is $k(\mathfrak{s}_1, \dots, \mathfrak{s}_s)$.

Recall that the dihedral invariants are defined as follows

$$\begin{aligned}\mathfrak{s}_1 &= a_1^{s+1} + a_s^{s+1} \\ \mathfrak{s}_2 &= a_1^{s-1} a_2 + a_s^{s-1} a_{s-1} \\ &\dots \\ \mathfrak{s}_i &= a_1^{s+1-i} a_i + a_s^{s+1-i} a_{s+1-i} \\ &\dots \\ \mathfrak{s}_{s+1-i} &= a_1^i a_{s+1-i} + a_s^i a_i \\ &\dots \\ \mathfrak{s}_{s-1} &= a_1^2 a_{s-1} + a_s^2 a_2 \\ \mathfrak{s}_s &= 2a_1 a_s\end{aligned}$$

Notice that these invariants are homogenous polynomials of degree $s+1$ to 2 respectively. The field of moduli of the corresponding curve is given by $k(\mathfrak{s}_1, \dots, \mathfrak{s}_s)$. Our goal is to find a Weierstrass equation over $k(\mathfrak{s}_1, \dots, \mathfrak{s}_s)$ of the curve in Eq. (1).

We perform a coordinate change

$$x \rightarrow \sqrt[s]{a_s} x$$

to get

$$y^n = a_s^{s+1} x^{\delta(s+1)} + a_s^{s+1} x^{\delta s} + a_{s-1} \cdot a_s^{s-1} x^{\delta(s-1)} + \dots + a_2 \cdot a_s^2 x^{\delta \cdot 2} + a_1 a_s x^{\delta} + 1$$

Denote by $A := a_s^{s+1}$. Then we have

$$2^{s+1} A^2 - 2^{s+1} \mathfrak{s}_1 A + \mathfrak{s}_s^{s+1} = 0.$$

This quadratic has discriminant

$$\Delta_s = 2^{s+1} (2^{s+1} \mathfrak{s}_1^2 - 4 \mathfrak{s}_s^{s+1})$$

The equation of the curve becomes

$$y^n = A x^{\delta(s+1)} + A x^{\delta s} + \sum_{i=1}^{s-1} a_i a_s^i \cdot x^{\delta \cdot i} + 1$$

We will show that all coefficients $a_i a_s^i$, $i = 1, \dots, s-1$, can be expressed in terms of the dihedral invariants and A . Hence, we have an equation of the curve over the quadratic extension $k\sqrt{\Delta_s}$.

Theorem 1. *Let \mathcal{X} be a genus $g \geq 2$ superelliptic curve, defined over \mathbb{C} , with an extra automorphism, $\mathfrak{s}_1, \dots, \mathfrak{s}_g$ its dihedral invariants, F the field of moduli, and K its minimal field of definition. Then, the following are true*

- i) *The minimal field of definition K is $K = F(\sqrt{\Delta_s})$*
- ii) *The equation of \mathcal{X} over K is*

$$(2) \quad y^n = A x^{\delta(s+1)} + A x^{\delta s} + \sum_{i=1}^{s-1} 2^{s-i} \mathfrak{s}_1 \cdot \frac{\mathfrak{s}_s^i \mathfrak{s}_i - A \mathfrak{s}_{s+1-i}}{2^s \mathfrak{s}_1^2 - \mathfrak{s}_s^{s+1}} \cdot x^{\delta \cdot i} + 1$$

where

$$2^{s+1} A^2 - 2^{s+1} \mathfrak{s}_1 A + \mathfrak{s}_s^{s+1} = 0.$$

Proof. Part i) is an immediate consequences of the above. To prove part ii) we have to express the coefficients $a_i a_s^i$ of $x^{\delta \cdot i}$, $i = 2, \dots, s-1$, in terms of $\mathfrak{s}_1, \dots, \mathfrak{s}_s$. From the definitions of \mathfrak{s}_i we get the following equations:

$$\begin{cases} \mathfrak{s}_1 = a_1^{s+1} + a_s^{s+1} \\ \mathfrak{s}_s = 2a_1 a_s \\ \mathfrak{s}_i = a_1^{s+1-i} a_i + a_s^{s+1-i} a_{s+1-i} \\ \mathfrak{s}_{s+1-i} = a_1^i a_{s+1-i} + a_s^i a_i \\ A = a_s^{s+1} \end{cases}$$

We multiply both sides in the definition of \mathfrak{s}_i by $a_s^i a_1^i = \left(\frac{\mathfrak{s}_s}{2}\right)^i$ and have

$$(3) \quad \left(\frac{\mathfrak{s}_s}{2}\right)^i \mathfrak{s}_i = a_1^{s+1} \cdot a_i \cdot a_s^i + a_s^{s+1} \cdot a_1^i \cdot a_{s+1-i}$$

From the definition of \mathfrak{s}_{s+1-i} we have

$$a_1^i a_{s+1-i} = \mathfrak{s}_{s+1-i} - a_i a_s^i,$$

which we substitute in the Eq. (3). Hence,

$$\boxed{a_i a_s^i = \frac{1}{a_1^{s+1} - a_s^{s+1}} \left(\frac{\mathfrak{s}_s^i}{2^i} \mathfrak{s}_i - A \mathfrak{s}_{s+1-i} \right)}$$

Denote by $B := a_1^{s+1} - a_s^{s+1}$. Notice that

$$\begin{aligned} (a_1^{s+1} - a_s^{s+1}) (a_1^{s+1} + a_s^{s+1}) &= a_1^{2(s+1)} - a_s^{2(s+1)} \\ &= a_1^{2(s+1)} + 2(a_1 a_s)^{s+1} + a_s^{2(s+1)} - 2(a_1 a_s)^{s+1} \\ &= (a_1^{s+1} + a_s^{s+1})^2 - 2 \left(\frac{\mathfrak{s}_s}{2}\right)^{s+1} \\ &= \mathfrak{s}_1^2 - \frac{1}{2^s} \mathfrak{s}_s^{s+1} \end{aligned}$$

Hence, $B \mathfrak{s}_1 = \mathfrak{s}_1^2 - \frac{1}{2^s} \mathfrak{s}_s^{s+1}$ and

$$B = \mathfrak{s}_1 - \frac{1}{2^s} \frac{\mathfrak{s}_s^{s+1}}{\mathfrak{s}_1},$$

provided that $\mathfrak{s}_1 \neq 0$.

Hence,

$$a_i a_s^i = 2^{s-i} \mathfrak{s}_1 \cdot \frac{\mathfrak{s}_s^i \mathfrak{s}_i - A \mathfrak{s}_{s+1-i}}{2^s \mathfrak{s}_1^2 - \mathfrak{s}_s^{s+1}}$$

as claimed. This completes the proof. \square

The natural question is for what values of $\mathfrak{s}_1, \dots, \mathfrak{s}_s$ is

$$\Delta_{\mathfrak{s}} = 2^{s+1} (2^{s+1} \mathfrak{s}_1^2 - 4 \mathfrak{s}_s^{s+1})$$

a complete square in K . In this case the field of moduli would be equal to the field of definition.

REFERENCES

- [1] T. Shaska, *Some Remarks on the Hyperelliptic Moduli of Genus 3*, Comm. Algebra **42** (2014), no. 9, 4110–4130.
- [2] T. Shaska and F. Thompson, *Bielliptic curves of genus 3 in the hyperelliptic moduli*, Appl. Algebra Engrg. Comm. Comput. **24** (2013), no. 5, 387–412.
- [3] T. Shaska, L. Beshaj, and Shor. C., *On Jacobian of curves with superelliptic components*, Contemporary Math. (to appear).
- [4] Lubjana Beshaj, Valmira Hoxha, and Tony Shaska, *On superelliptic curves of level n and their quotients, I*, Albanian J. Math. **5** (2011), no. 3, 115–137.
- [5] Tony Shaska and Fred Thompson, *Equations over the minimal field of definition for superelliptic curves, II*, work in progress.
- [6] Tanush Shaska, *Determining the automorphism group of a hyperelliptic curve*, Proceedings of the 2003 International Symposium on Symbolic and Algebraic Computation, ACM, New York, 2003, pp. 248–254 (electronic), DOI 10.1145/860854.860904, (to appear in print). MR2035219 (2005c:14037)
- [7] Jean-Francois Mestre, *Construction de courbes de genre 2 à partir de leurs modules*, Effective methods in algebraic geometry (Castiglioncello, 1990), Progr. Math., vol. 94, Birkhäuser Boston, Boston, MA, 1991, pp. 313–334 (French). MR1106431 (92g:14022)
- [8] Jannis A. Antoniadis and Aristides Kontogeorgis, *On cyclic covers of the projective line*, Manuscripta Math. **121** (2006), no. 1, 105–130.
- [9] J. Gutierrez and T. Shaska, *Hyperelliptic curves with extra involutions*, LMS J. Comput. Math. **8** (2005), 102–115.
- [10] R. Sanjeewa and T. Shaska, *Determining equations of families of cyclic curves*, Albanian J. Math. **2** (2008), no. 3, 199–213.
- [11] Christopher Towse, *Weierstrass weights of fixed points of an involution*, Math. Proc. Cambridge Philos. Soc. **122** (1997), no. 3, 385–392, DOI 10.1017/S0305004197001837. MR1466643 (98i:14033)